

ATTACHMENT 8

DD FORM 254

CONTRACT SECURITY CLASSIFICATION SPECIFICATION

DATE: 18 March 2009
(Supersedes DD 254 dated 17 September 2008)

This Document contains information EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS (b)(4) and (b)(5) apply.

FOR OFFICIAL USE ONLY

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort)

1. CLEARANCE AND SAFEGUARDING

a FACILITY CLEARANCE REQUIRED

TOP SECRET

b LEVEL OF SAFEGUARDING REQUIRED

SECRET

2. THIS SPECIFICATION IS FOR (x and complete as applicable)

X	a PRIME CONTRACT NUMBER	FA8808-06-C-0001
	b SUBCONTRACT NUMBER	
	c SOLICITATION OR OTHER NUMBER	
	Due Date (YYMMDD)	

3. THIS SPECIFICATION IS: (x and complete as applicable)

a ORIGINAL (Complete date in all cases)	Date (YYMMDD)
	060607
b REVISED (Supersedes all previous specs)	Revision No
	4
c FINAL (Complete Item 5 in all cases)	Date (YYMMDD)
	090318

4. IS THIS A FOLLOW-ON CONTRACT?

☐ YES ☒ NO

If Yes, complete the following

Classified material received or generated under

(Preceding Contract Number) is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254?

☐ YES ☒ NO

If Yes, complete the following:

In response to the contractor's request dated

retention of the identified classified material is authorized for the period of

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a NAME, ADDRESS, AND ZIP CODE	b CAGE CODE	c COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) SEE NEXT PAGE FOR LIST OF COGNIZANT SECURITY OFFICES
Boeing Satellite Systems, Inc. 2260 E. Imperial Highway El Segundo, CA 90245	9E831	Defense Security Services (S41HB) One Pacific Plaza 7777 Center Drive, Suite 260 Huntington Beach, CA 92647-9109

7. SUBCONTRACTOR

a NAME, ADDRESS, AND ZIP CODE	b CAGE CODE	c COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

8. ACTUAL PERFORMANCE

a LOCATION	b CAGE CODE	c COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
Boeing Satellite Systems, Inc. 2260 E. Imperial Highway El Segundo, CA 90245	9E831	Defense Security Services (S41HB) One Pacific Plaza 7777 Center Drive, Suite 260 Huntington Beach, CA 92647-9109

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

United States Air Force Wideband Global Satellite Communications Program

10. THIS CONTRACT WILL REQUIRE ACCESS TO:

YES NO

a COMMUNICATIONS SECURITY (COMSEC) INFORMATION

☒

b. RESTRICTED DATA

☐

c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

☒

d FORMERLY RESTRICTED DATA

☒

e. INTELLIGENCE INFORMATION:

☐

(1) Sensitive Compartmented Information (SCI)

☐

(2) Non-SCI

☒

f. SPECIAL ACCESS INFORMATION

☐

g NATO INFORMATION

☐

h FOREIGN GOVERNMENT INFORMATION

☐

i LIMITED DISSEMINATION INFORMATION

☐

j FOR OFFICIAL USE ONLY INFORMATION

☒

k OTHER (Specify)

Contractor to be in compliant with Public Key Infrastructure (PKI)

☒

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:

YES NO

a HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY

☐

b RECEIVE CLASSIFIED DOCUMENTS ONLY

☒

c RECEIVE AND GENERATE CLASSIFIED MATERIAL

☒

d FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE

☒

e PERFORM SERVICES ONLY

☒

f HAVE ACCESS TO US CLASSIFIED INFORMATION OUTSIDE THE US, PUERTO RICO, US POSSESSIONS AND TRUST TERRITORIES

☒

g BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CTR

☒

h REQUIRE A COMSEC ACCOUNT

☒

i HAVE TEMPEST REQUIREMENTS

☒

j HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS

☒

k BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE

☒

l OTHER (Specify)

☒

1. Be authorized unclassified Automated Information Process with DoD unclassified National Security Information

☒

2. Have access to DoD PKI sites

☒

12. **PUBLIC RELEASE.** Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate US Government authority. Proposed public release shall be submitted for approval prior to release

☐ Direct ☒ Through (Specify):

The contractor shall refer to the WGS SCG and the WGS Contracting Officer for procedures regarding the release of program information to the general public, to foreign entities, to US citizens, foreign nationals residing in foreign countries, or to news organizations. Release of information must be approved by SMC/PA at the address below, and the WGS program office.

SMC/PA
483 N. Aviation Boulevard
El Segundo, CA 90245-2808

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. **SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

A. Contractor will comply with DoD 5220.22M, National Industrial Security Program Operating Manual (NISPOM), National Security Agency Central Security Service (NSA/CSSM) Manual 3-16 and DoD 5200.1-R Information Security Program (Appendix 3).

B. Security Guidance for this effort is governed by the Wideband Global Satellite Communications (WGS) Program Security Classification Guide (SCG) dated 18 March 2008. This includes updates/revisions as directed in Executive Order (E.O.) 13292. For any conflicts, challenges and/or questions regarding this guidance contact the MILSATCOM Systems Wing, MCSW/OM, 483 N. Aviation Blvd., El Segundo, CA 90245

C. The contractor shall protect Critical Program Information (CPI), technologies, and systems, when identified in the WGS Protection Plan (PPP). Currently no CPI are identified. If identified in the future, the engineering change proposal (ECP) process via MILSATCOM Change Board (MCB) will be used to effect change to the contract. Physical protection level of CPI is based in its classification and protected IAW NISPOM requirements. CPI's maintained in electronic or printed form will be protected as FOUO unless otherwise directed in the PPP.

D. Review of this DD 254 is required biannually.

Special Security Officer
SMC/IN

Industrial Security Program Officer
SMC/PIP

Chief, Security and Protection
MILSATCOM Systems Wing

14. **ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the Requirements to the cognizant security office. Use items 13 if additional space is needed.)

☒ Yes ☐ No

See attachment(s) for additional security guidance.

15. **INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas of elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

☒ Yes ☐ No

Contractors, while on Government/Military installations, will comply with the Base organizational security and/or protection requirements. The Defense Security Service is relieved of inspection responsibility while on a Government/Military installation, unless requested. MCSW/OM will conduct a Program Protection Survey of contractor facilities, as required through each phase of the life cycle.

16. **CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

b. TITLE

Contracting Officer

c. TELEPHONE (Include Area Code)

d. ADDRESS (Include Zip Code)

MCSW/PK
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

17. **REQUIRED DISTRIBUTION**

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR |
| <input type="checkbox"/> | b. SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input type="checkbox"/> | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input checked="" type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER |
| <input checked="" type="checkbox"/> | f. OTHERS AS NECESSARY (SMC/PIP, SMC/INS, SMC/MCK) |

Reference Block: 10a – Communications Security (COMSEC) Information

1. The Contractor is authorized access to COMSEC information and will comply with National Security Agency Central Security Service NSA/CSS Policy Manual No.3-16 (replaced NSA Manual 90-1.) Access to COMSEC material/information is restricted to U.S. citizens who have been briefed according to the NISPOM and possess an approved government clearance. NOTE: The COMSEC/CRYPTO briefing applies only to the use and control of CRYPTO equipment and specialized COMSEC publications.
2. The Contractor shall adhere to guidance regarding Two Person Integrity contained in an attachment to this attachment immediately following.
3. NACSIM/NACSEM documents are not considered COMSEC controlled material. Additionally, cryptographic information/equipment shall be retained in a Contractor facility COMSEC account.

Reference Block: 10e(2) Intelligence Information – Non-Sensitive Compartmented Information

(2) Non-SCI

Provisions for the handling of Non-SCI or “Collateral” Intelligence by contractors is governed by Chapter 9, Section 3 of DoD 5220.22-M, the National Industrial Security Program Operating Manual, 2006 (NISPOM). Particular emphasis is placed on the contractor(s) correctly understanding and heeding intelligence portion markings.

As classified material, collateral intelligence will be afforded the same protections, safeguards and precautions required by any classified material unless special intelligence related handling instructions are additionally imposed. These basic safeguards are found in DoD 5200.1-R, Information Security Program and AFI 31-401, Information Security Program Management. The disclosure or release of intelligence derived information, whether its status is collateral or SCI, is not authorized without the prior consent of SMC/IN.

Reference Block 10j – For Official Use Only Information (FOUO)

See Reference Block 13. FOUO Guidance in accordance with Security Classification Guide’s (SCG’s).

FOR OFFICIAL USE ONLY (FOUO) information will be handled as follows:

1.0 General.

1.1 For Official Use Only (FOUO) is official government information that does not meet requirements for classification but still requires protection. By definition, information shall be unclassified in order to be designated FOUO. If an item of classified information is declassified, it may be designated FOUO if it qualifies under one of the other exemptions of the FOIA. This means that:

1.1.1 Information cannot be classified and FOUO at the same time. Therefore, classified documents containing FOUO information cannot bear an overall document marking of FOUO. However, portions or pages of a classified document, that contain only FOUO information will be marked as FOUO.

1.1.2 Information that is declassified may be designated FOUO, only if it is believed to fit into one or more of the last eight exemptions (exemptions 2 through 9).

1.2 FOUO information may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (5 USC 552). Most FOUO information generated or handled in support of this contract will be exempt from mandatory disclosure under exemptions 4 and 5.

1.3 FOUO information may be released to the public; however, the Government prior to its release must review it. Information in support of this contract must be reviewed by SMC/PA prior to release.

2.0 Identification Markings.

2.1 An unclassified document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the outside of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside back cover (if any). For convenience, all pages, even those that do not contain FOUO information may be marked in documents generated by automated systems.

2.2 Portion Marking FOUO Information. Subjects, titles and each section, part, paragraph, and similar portion of an FOUO document shall be marked to show that they contain information requiring protection. Use the parenthetical notation "(FOUO)" to identify information as For Official Use Only for this purpose. Place this notation immediately before the text.

2.3 Individual pages within a classified document that contain both FOUO and classified information will be marked top and bottom with the highest security classification of information appearing on the page. Individual portions/paragraphs containing FOUO information but no classified information will be marked "FOUO."

2.4 Marking information FOUO does not automatically qualify it for exemption. If a request for a record is received, the information shall be reviewed to determine if it actually qualifies for exemption. Similarly, the absence of the FOUO marking does not automatically mean the information shall be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still be withheld under the FOIA. All DoD unclassified information must be reviewed before it is released to the public or to foreign governments and international organizations.

2.4.1 The cover or the first page of unclassified documents containing FOUO information will be marked with the following statement:

This Document contains information EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS (b)(4) and (b)(5) apply.

2.5 Certain classified material on this contract may be downgraded by the Original Classification Authority to FOUO or may be automatically declassified under E.O. 12958 as Amended. When classified material approved for declassification to FOUO is used, extracted, reissued, transmitted and/or updated, it must be reviewed and appropriately marked.

3.0 Access to FOUO Information.

3.1 No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.

3.2 The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge or control of the information and not on the prospective recipient.

3.3 Information designated as FOUO may be disseminated within the DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense, provided that dissemination is not further controlled by a Distribution Statement.

3.4 DoD holders of information designated as FOUO are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a government function. If the information is covered by the Privacy Act, disclosure is only authorized if the requirements of DoD 5400.11-R are satisfied.

3.5 Release of FOUO information to Congress is governed by DoD Directive 5400.4. If the information is covered by the Privacy Act, disclosure is authorized if the requirements of DoD 5400.11-R are also satisfied.

3.6 DoD Directive 7650.1 governs release of FOUO information to the General Accounting Office (GAO). If the information is covered by the Privacy Act, disclosure is authorized if the requirements of DoD 5400.11-R are also satisfied.

4.0 Transmission/Dissemination/Reproduction.

4.1 Authorized contractors, consultants, and grantees may transmit/disseminate FOUO information internally to each other and to DoD components and officials of DoD components who have a legitimate need for the information in connection with this contract. The following guides apply:

4.1.1 FOUO information may be discussed over non-secure telephones and other electronic instruments. Cordless, cellular and mobile telephones should be avoided.

4.1.2 FOUO information may be transmitted over non-secure facsimile equipment.

4.1.3 Documents of facsimile transmissions containing FOUO material or with FOUO material attached must be marked to identify any FOUO contents or attachments.

4.1.4 FOUO information and material may be transmitted via first class mail, parcel post or, for bulk shipments, via fourth class mail. Electronic transmission of FOUO information, e.g., voice,

data or facsimile, e-mail, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI), whenever practical.

4.1.4.1 FOUO information may be transmitted, processed, and stored on Automated Information Systems (AIS), electronic mail, and other similar systems or networks (1) when distribution is to an authorized recipient and (2) if the receiving system is protected by either physical isolation or a password protection system. Holders will not use general, broadcast, or universal mail addresses to distribute FOUO information. Discretionary access control measures may be used to preclude access to FOUO files by users who are authorized system users but are not authorized for FOUO information.

4.1.4.2 FOUO information may only be posted to DoD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum dated December 1998, Subject: "Web Site Administration".

4.1.5 Reproduction of FOUO information may be accomplished on unclassified copiers or within designated government or contractor reproduction areas.

5.0 Protection of FOUO Information.

5.1 During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. FOUO information must be stored in locked desks, file cabinets, bookcases, locked rooms, etc. after working hours.

6.0 Disposition.

6.1 Record copies of FOUO documents shall be disposed of according to the Federal Records Act and the DoD Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information, e.g. by shredding and placing in a recycle or trash container or by initializing, degaussing, or shredding magnetic media.

6.2 FOUO material may be recycled. Safeguard the FOUO documents or information until recycled. Recycling contracts must include on how to protect and destroy FOUO material.

6.3 Removal of the FOUO status can only be accomplished by the government originator of the information. SMC/PA will review and/or coordinate the removal of FOUO status for SMC information in support of this contract.

7.0 Unauthorized Disclosure.

7.1 The unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DoD information classified for security purposes. However, appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DoD Component that originated the FOUO information, i.e. the contracting officer, shall be informed of its unauthorized disclosure.

Reference Block 10k – (Other) Public Key Infrastructure

A PKI Public Key Infrastructure (PKI) enables users of an unsecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure assumes the use of *public key cryptography*, which is the most common method on the Internet for authenticating a message sender or encrypting a message.

Reference Block: 11c – Receive And Generate Classified Material

Classified material will be handled in accordance with guidance in the NISPOM and E.O. 13292.

Reference Block: 11d – Fabricate, Modify, or Store Classified Hardware

The Contractor is required to provide storage to the level of (SECRET) for classified hardware that, due to size or quantity, cannot otherwise be safeguarded in GSA approved storage containers.

Reference Block: 11f – Access to Classified Information Outside the U.S

Contractor requires access to U.S. Classified Information outside the U.S. Possession and Trust Territories.

The User Agency HQ, Space and Missile Systems Center will furnish complete classification guidance for the service to be performed. The highest level of classification for the contract is SECRET.

Reference Block: 11g – Be Authorized to Use the Services of Defense Technical Information Center (DTIC) or Other Secondary Distribution Center

The contractor is required to obtain proper access to classified material. See NISPOM Chapter 11, Section 2 for more information.

Reference Block: 11h – Require a COMSEC Account

NSA account will be established for and maintained by contractor IAW NSA/CSS Manual 3-16. The Contractor will comply with the additional security requirements and the management of NSA information/material as defined in the manual.

Reference Block: 11j – OPSEC Requirements

The contractor will accomplish the following minimum requirements in support of the User Agency Operations Security (OPSEC) Program.

Items of critical information are those facts, which individually, or in the aggregate, reveal sensitive details about the contractor's security operations, and thus require protection from adversarial collection or exploitation.

Include OPSEC as a part of its ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the NISPOM and Chapter 3 of AFI 10-701; as applicable.

Protect items on the critical information list (CIL) contained in the MCSW OPSEC Plan and determine applicable to contractor operations. Be responsive to the User Agency OPSEC Manager (MCSW/OM) on a non-interference basis. Protect sensitive unclassified information and activities, which could compromise classified information or operations, or degrade the planning and execution of military operations performed by the contractor in support of the mission. Sensitive unclassified information is that Information marked **FOR OFFICIAL USE ONLY**, Privacy Act Of 1974, **COMPANY PROPRIETARY**, and as identified by the Air Force Program Office and the MCSW/OM OPSEC Manager.

Reference Block: 11k – Authorized Use of Defense Courier Service

Use of Defense Courier Service for the required COMSEC account is authorized. The facility Security Officer (FSO), COMSEC account manager, or an authorized representative will prepare and submit DCS Form 10 in original triplicate to the appropriate DSC station.

Reference Block 11l – Other

(1) For all Unclassified Automated Information Systems (AIS) processing, storing, displaying, or transmitting of “Unclassified Government National Security Information (NSI) in support of MCSW, all necessary actions should be taken to ensure the integrity, confidentiality, and protection of said NSI from unauthorized personnel.

This shall include such methods as password protection, encryption, locking computer screens or logging out of systems, similar to contractor’s process for protecting proprietary information. Said methods shall be in accordance with the contractor’s approved Command Media, a copy of which shall be forwarded to MCSW/OM.

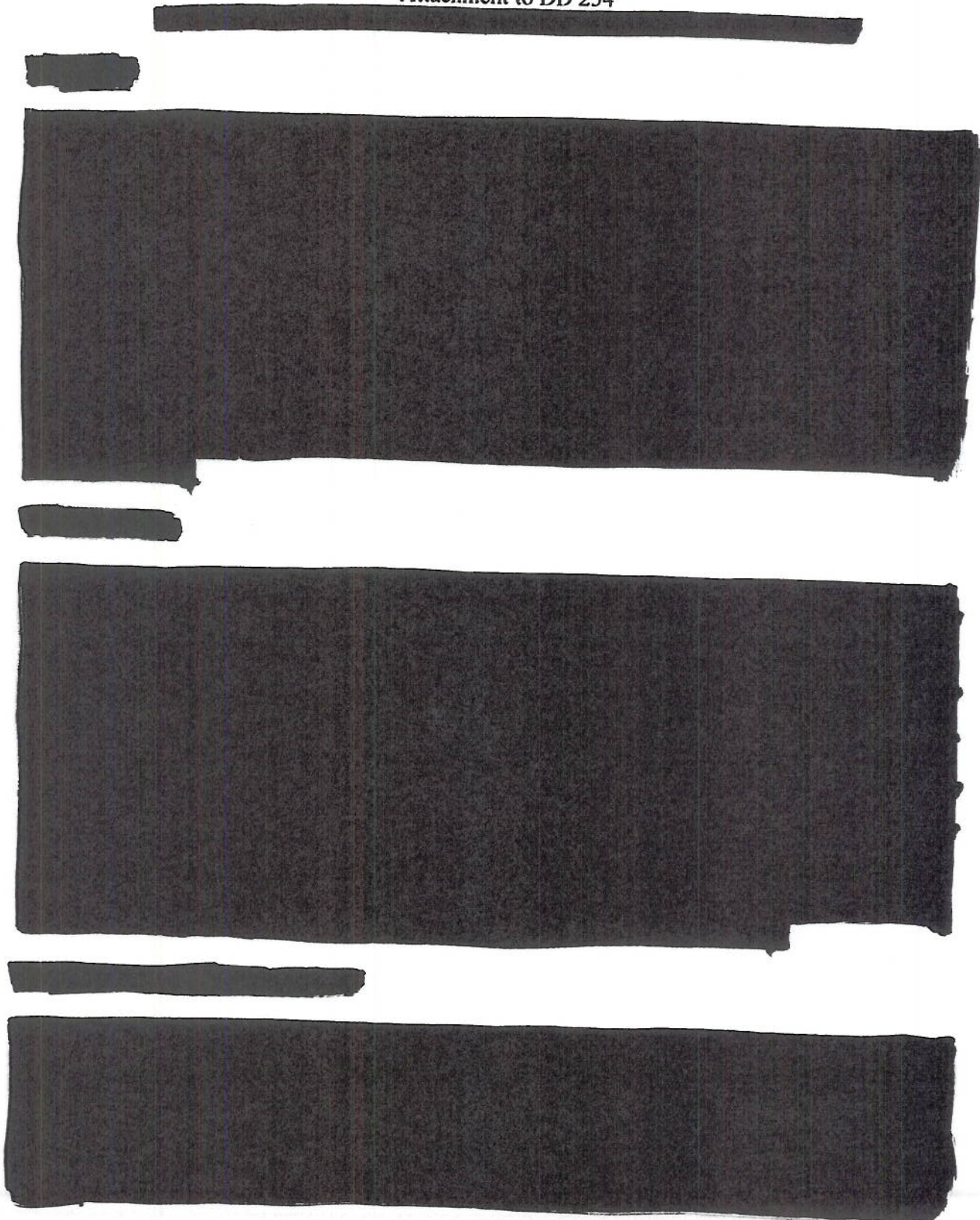
(2) Organization that require access to DoD website will be required to be Public Key Infrastructure (PKI) compliant. DoD approved commercial certificates for their users requiring access to DoD websites can be obtained from <http://iase.disa.mil/pki/eca/index.html>

BLOCK 14: Additional Security Requirements:

The contractor shall comply with the general security provisions of the following documents, including changes or revisions.

- 1 DoD 5400.7-R/AF Sup, 24 June 2002, DoD Freedom Of Information Act Program
- 2 DoDD 5200.39, 10 Sep 97, Security Intelligence, and Counterintelligence Support to Acquisition Program Protection.
- 3 DoD 5220.22-M, Feb 2006, National Industrial Security Program Operating Manual (NISPOM) and subsequent changes or revisions.

Attachment to DD 254

The page contains several large rectangular areas of redacted content, represented by solid black blocks. These redactions cover the majority of the page's body text, leaving only the header, footer, and a small section of the left margin visible.

FA8808-06-C-0001
Attachment 8 (DD254)
Page 11 of 14

FOR OFFICIAL USE ONLY

A dark, textured rectangular object, possibly a book cover or a piece of fabric, with a lighter, possibly metallic, strip along the right edge. The object is oriented horizontally and occupies most of the frame. The texture appears grainy or woven. The right edge shows a distinct vertical line where the material meets a lighter strip.



[REDACTED]

[REDACTED]



A long, narrow, dark, textured object, possibly a piece of fabric or a book cover, with a vertical crease or fold in the center. The texture appears fibrous or woven. There are some faint vertical lines or creases visible, particularly on the left side. The object is set against a plain white background.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]